

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

**IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH APPLE  
ICLOUD ACCOUNT  
METHODSOFMAYHEM@ICLOUD.COM  
AND THE APPLE ID  
METHODSOFMAYHEM@METROCAST.NET**

**Case No. 24-mj-67-01/02-TSM**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Tarah E. Snee, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. (“Apple” or “PROVIDER”), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B, using the procedures described in Section III of that attachment.

2. I have been employed as an FBI Special Agent since 2015, and am currently assigned to the Boston Field Office, Bedford Resident Agency. I am a federal law enforcement

officer who is engaged in enforcing criminal laws, including 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(2) related to the possession and distribution of child pornography in the District of New Hampshire. I have investigated federal criminal violations related to high technology or cyber-crime, child exploitation, and child pornography. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

#### **STATUTORY AUTHORITY**

4. This investigation concerns alleged violations of 18 U.S.C. § 2252(a)(4)(B) and 18 U.S.C. § 2252A(a)(2), related to the possession and distribution of child pornography in the District of New Hampshire. 18 U.S.C. § 2252(a)(4)(B) makes it a crime for any person to knowingly possess one or more images depicting a minor under the age of 18 engaged in sexually explicit conduct. 18 U.S.C. § 2252A(a)(2) makes it a crime for any person to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

#### **PROBABLE CAUSE**

5. On July 20, 2023, an Online Covert Employee with the United Kingdom South East Regional Crime Unit (hereafter referred to as OCE#1) posing as a 13 year-old female

received a direct message on the Kik platform from Kik user “jm42043” who asked “How old are you?”, “Are you 13?”. On July 22, 2023 “jm42043” sent to OCE#1 an image of an adult male’s erect penis. The following conversation between “jm42043” and OCE#1 then occurred:

OCE#1: hey yeh im 13 how u know that x

JM42043: I guessed

JM42043: You like my dick?

OCE#1: lol dunno not see many x

JM42043: Got any sisters?

OCE#1: nah whys that x

JM42043: Any little cousins?

OCE#1: yeh why x

JM42043: How old?

OCE#1: 6 and 9

JM42043: Do you think the 9 year old would want to see a man’s dick?

[LATER IN THE CONVERSATION]

OCE#1: how old r u and wheres u from x

JM42043: I’m 43 and USA do you think she’d want to see my dick?

JM42043: You look like you’re 11 btw

6. “jm42043” proceeded to send messages from July 31, 2023 until August 6, 2023 that went unanswered by OCE#1 including:

JM42043: I bet both your cousins would like seeing my dick

JM42043: Do you think your 9 year old cousin would want to fuck?

JM42043: I would fuck her real good and cum in her

JM42043: I would fuck and cum in the 6 year old too

7. On August 7, 2023, pursuant to an administrative subpoena, Kik provided the following subscriber information for user “jm42043”: First Name: J Last Name: M Email: [methodsofmayhem@icloud.com](mailto:methodsofmayhem@icloud.com). The IP address 65.175.240.91, which resolved to Breezeline, was used by “jm42043” to access Kik on various dates during the timeframe of the chats between the target Kik user and OCE#1.

8. On August 30, 2023, pursuant to an administrative subpoena, Breezeline provided the following subscriber information for the IP address 65.175.240.91 during the relevant timeframe:

Name: Kathleen Murphy

Address: [REDACTED]

Associated Phone Numbers: (603) 755-6883, (603) 312-4752, (603) 923-1028

Email address: katm811@metrocast.net, disturbed@metrocast.net, murphys@metrocast.net, methodsofmayhem@metrocast.net.

9. An open-source search for the phone number (603) 923-1028, provided by Breezeline as associated with the target IP address, yielded a Snapchat account for Michael Murphy with the username “methods0fmayhem”.

10. From November 14, 2023, to November 16, 2023 an Online Covert Employee with the United Kingdom South East Regional Crime Unit (hereafter referred to as OCE#2) posing as a 12 year-old female received a direct message on the Kik platform from Kik user “mm12480” asking their age and if they were 10 years old. “mm12480” proceeded to send OCE#2 an image of an adult male’s erect penis. The following conversation between “mm12480” and OCE#2 occurred:

MM12480: Want to fuck?

OCE#2: Lik I dnt no u...

MM12480: So

MM12480: I'll cum in you

MM12480: Want to feel my huge dick in you?

MM12480: Want to suck my huge dick for me?

MM12480: Nobody would know you fucked a man

[LATER IN THE CONVERSATION]

MM12480: I fucked 10 year olds and we didn't know each other

OCE#2: Where u frm? How old u? Wat ur name...c I I no u

MM12480: So what who cares those other girls just wanted my dick in them

11. On December 18, 2023, pursuant to an administrative subpoena, Kik provided the following subscriber information for Kik user "mm12480":

First Name: mm12480

Email: [methodsofmayhem@icloud.com](mailto:methodsofmayhem@icloud.com)

Kik also advised that the IP address used by "mm12480" to access the Kik account was 65.175.240.91. This is the same IP address previously identified by Kik as having been used by Kik user "jm42043" during the chats with OCE#1.

12. On February 2, 2024, pursuant to an administrative subpoena, Breezeline provided the following subscriber information for the IP address 65.175.240.91 during the timeframe of the chats between Kik user "mm12480" and OCE#2:

Name: Kathleen Murphy

Address: [REDACTED]

Associated Phone Numbers: (603) 755-6883, (603) 312-4752, (603) 923-1028

13. On December 12, 2023 an investigator from the Office of the Idaho Attorney General's (OAG) Internet Crimes Against Children (ICAC) Unit (hereafter referred to OCE#3) posing as a 12-year-old female on Kik received a direct message from "mm12480". The following conversation took place:

MM12480: I fucked some pretty young girls too

OCE#3: cool

OCE#3: did they like it

MM12480: Some of the older ones who were young did

OCE#3: oh kool

MM12480: She was 9

OCE#3 and "mm12480" had multiple conversations between December 12, 2023 and December 27, 2023. On December 27, 2023, "mm12480" asked OCE#3 "Want to see my daughter taking my dick?". User "mm12480" then sent a 31-second video depicting a prepubescent minor female approximately nine years old laying on her back being vaginally penetrated by an adult male's penis. Law enforcement subsequently submitted this video to the National Center for Missing and Exploited Children (NCMEC), which in turn advised that this video depicts a known (i.e., previously identified) minor victim.

14. Pursuant to an administrative subpoena, Kik provided the following email address for Kik user "mm12480" on the date the video was sent: [methodsofmayhem@icloud.com](mailto:methodsofmayhem@icloud.com). An IP address associated with the account, 65.175.240.91, resolved to Breezeline, and was the same IP address used by the target Kik users in conversations with OCE#1 and OCE#2.

15. Pursuant to an administrative subpoena, Breezeline provided the following subscriber information for the IP address 65.175.240.91 on the date that “mm12480” sent the video described above to OCE#3:

Name: Kathleen Murphy

Address: [REDACTED]

Phone Number: (603) 755-6883, (603) 312-4752, (603) 923-1028

16. On February 14, 2024 pursuant to an administrative subpoena, Apple provided the following subscriber information for [methodsofmayhem@icloud.com](mailto:methodsofmayhem@icloud.com), which was the email address associated with both the “jm42043” and “mm12480” Kik accounts:

First Name: Michael

Last Name: Murphy III

Account Status: Active

Address: [REDACTED]

Phone Number: (603) 312-4752, (603) 923-1028

17. On December 29, 2023, a search warrant was served on Kik username “mm12480” by the Idaho OAG ICAC. The contents of the search warrant were received and reviewed by FBI Boston/Bedford RA on February 14, 2024. The account contained six videos and two images depicting CSEM, including the video that was sent to OCE#3 on December 27, 2023. It also included the pictures sent to OCE#1 and OCE#2 depicting an adult male’s penis and multiple chats between “mm12480” and various Kik users. In the chats, “mm12480” made statements to other Kik users such as, “we can make child porn”, “I’ve had sex with little girls like you before”, and “Got any little girls between 5 and 10 being raped by her dad?”

18. Through an inquiry of open search databases and the New Hampshire Department of Safety – Division of Motor Vehicles (“DMV”) database, it was determined Michael F J Murphy III, resides at 61 Ivy Lane, Farmington, NH. Open source records also show Kathleen Murphy and Michael F J Murphy, Jr., who are married and appear to be Michael F J Murphy III’s parents, residing at the same address.

19. On February 22, 2024, a federal search warrant was executed at 61 Ivy Lane Farmington, NH, and on the person of Michael F J Murphy III (“Murphy”). During the course of the search, Murphy was advised that there was a federal search warrant for his person and home. Murphy was further advised that he was not under arrest. Murphy advised that he understood. Agents asked if Murphy would be willing to speak with them about the investigation, to which Murphy agreed. During the interview, Murphy confirmed he was the user of the black iPhone 15 seized during the search. He stated that he was the user of methodsofmayhem@icloud.com and methodsofmayhem@me.com. Murphy also disclosed that in the past he had saved videos and pictures depicting child sexual abuse material onto his iCloud account.

20. During a manual review of the defendant’s phone, the Apple ID presently signed into the device was methodsofmayhem@metrocast.net. In addition, in response to legal process, Apple provided several login aliases associated with the Apple ID methodsofmayhem@metrocast.net, to include methodsofmayhem@me.com and methodsofmayhem@icloud.com. Apple further identified the following iCloud features where data associated with the Apple ID methodsofmayhem@metrocast.net may be stored:



DSID	Apple ID	iCloud Feature	Feature Used
205623885	methodsofmayhem@metrocast.net	iCloud Backup (iOS Devices)*	Yes
205623885	methodsofmayhem@metrocast.net	Bookmarks*	Yes
205623885	methodsofmayhem@metrocast.net	Calendars	Yes
205623885	methodsofmayhem@metrocast.net	iCloud Photos*	Yes
205623885	methodsofmayhem@metrocast.net	Contacts	Yes
205623885	methodsofmayhem@metrocast.net	Find My Friends	Yes
205623885	methodsofmayhem@metrocast.net	iCloud Drive*	Yes
205623885	methodsofmayhem@metrocast.net	iCloud Reminders*	Yes
205623885	methodsofmayhem@metrocast.net	Mail	Yes
205623885	methodsofmayhem@metrocast.net	Mail Header	Yes
205623885	methodsofmayhem@metrocast.net	Maps	No
205623885	methodsofmayhem@metrocast.net	Messages in iCloud*	Yes
205623885	methodsofmayhem@metrocast.net	Notes*	Yes
205623885	methodsofmayhem@metrocast.net	Safari Browsing History	No
205623885	methodsofmayhem@metrocast.net	Sign in with Apple	Yes

### **BACKGROUND CONCERNING APPLE**<sup>1</sup>

21. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

22. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

---

<sup>1</sup> The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at [https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf), and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.
- c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple’s servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.
- d. Game Center, Apple’s social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to determine a user’s approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

23. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be

linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

24. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

25. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

26. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP

address and identifiers such as the Integrated Circuit Card ID number (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone number of a user’s iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

27. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user’s photos and videos, iMessages, Short Message Service (“SMS”) and Multimedia Messaging Service (“MMS”) messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple’s servers in an encrypted form but may nonetheless be decrypted by Apple. Records

and data associated with third-party apps, including the instant messaging service Kik, may also be stored on iCloud.

28. The stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

29. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services that may constitute evidence of the crimes under investigation.

### **CONCLUSION**

30. Based on the facts set forth above, there is probable cause to believe that Murphy has committed violations of possession and distribution of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and 18 U.S.C. § 2252A(a)(2) and there may be evidence of those crimes within his iCloud account. Accordingly, I respectfully request that this Court grant the attached application for a criminal complaint.

31. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ Tarah Snee

Tarah Snee



Special Agent

Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Apr 11, 2024

Time: 2:29 PM

HONORABLE TALESHA L. SAINT-MARC  
UNITED STATES MAGISTRATE

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with the Apple account(s) associated with [methodsofmayhem@icloud.com](mailto:methodsofmayhem@icloud.com) and the Apple ID [methodsofmayhem@metrocast.net](mailto:methodsofmayhem@metrocast.net), as well as information preserved from the account(s) pursuant to a request made under 18 U.S.C. § 2703(f) (see ref. # 202400511797), which is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company that is headquartered at / accepts service of legal process at One Apple Park Way, Cupertino, CA.



**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Apple Inc. (“PROVIDER”) to facilitate execution of the warrant**

To the extent that the information described in Attachment A is within the possession, custody, or control of PROVIDER, including any records that have been deleted but are still available to PROVIDER, PROVIDER is required to disclose the following information to the government corresponding to each account or identifier (the “Account”) listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all images, videos, device settings, and bookmarks;

d. All records and information regarding locations where the account or devices associated with the account were accessed from January 1, 2023 to February 22, 2024, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

e. All records pertaining to the types of service used;

f. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

g. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfo.txtfiles).

## **II. Information to be Seized by the Government**

All information described above in Section I that constitutes fruits, contraband, evidence, instrumentalities, and information relating to violations of 18 U.S.C. § 2252(a)(4)(B) and 18 U.S.C. § 2252A(a)(2), as described in the affidavit submitted in support of this warrant, including, for the account described in Attachment A, including information pertaining to the following matters:

A. The sexual abuse or exploitation of any child;

- B. The possession, distribution, receipt, or transportation of child pornography,
- C. The identity of persons who either (i) used or controlled the target account(s); (ii) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the Target Offense(s); or (iii) communicated with the account about matters relating to the Target Offense(s).

Apple is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the accounts, accounts status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MCA”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile

Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”) and International Mobile Station Equipment Identities (“IMEI”);

- c. All files and other records backed up to the iCloud related to iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, images, videos and bookmarks.

**I. Government procedures for warrant execution**

The United States government will conduct a search of the information produced by the PROVIDER and determine which information is within the scope of the information to be seized specified in Section II. That information that is within the scope of Section II may be copied and retained by the United States.

Law enforcement personnel will then seal any information from the PROVIDER that does not fall within the scope of Section II and will not further review the information absent an order of the Court. Such sealed information may include retaining a digital copy of all information received pursuant to the warrant to be used for authentication at trial, as needed.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
RECORDS PURSUANT TO FEDERAL RULES OF  
EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple Inc. ("Apple"), and my title is \_\_\_\_\_. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and

b. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature